JVCKenwood hit by Conti ransomware claiming theft of 1.5TB data

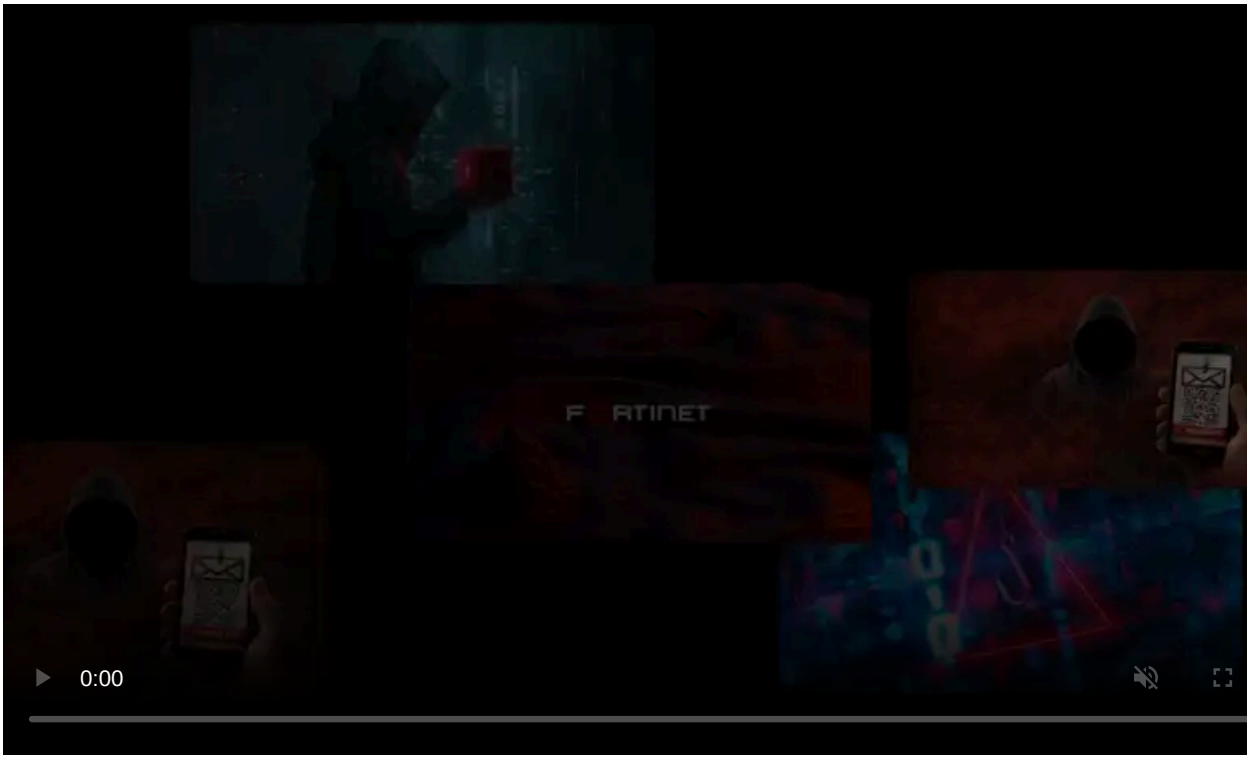
By Lawrence Abrams

Published: 2021-09-30 · Archived: 2026-04-06 03:23:24 UTC

JVCKenwood has suffered a Conti ransomware attack where the threat actors claim to have stolen 1.7 TB of data and are demanding a $7 million ransom.

JVCKenwood is a multinational electronics company based out of Japan that employs 16,956 people and has a 2021 revenue of $2.45 billion. The company is known for its brands JVC, Kenwood, and Victor, which manufacture car and home audio equipment, healthcare and radio equipment, professional and in-vehicle cameras, and portable power stations.

Yesterday, JVCKenwood disclosed that servers belonging to its sales companies in Europe were breached on September 22nd, and the threat actors may have accessed data during the attack.


F RTINET
0:00

"JVCKENWOOD detected unauthorized access on September 22, 2021 to the servers operated by some of the JVCKENWOOD Group's sales companies in Europe. It was found that there was a possibility of information leak by the third party who made the unauthorized access," JVCKENWOOD announced in a press statement.

"Currently, a detailed investigation is being conducted by the specialized agency outside the company in collaboration with the relevant authorities. No customer data leak has been confirmed at this time. The details will be announced on the company website as soon as they become available."

JVCKenwood hit by ransomware

Today, a source shared a ransom note for a CONTI ransomware sample used in the attack against JVCKenwood.

In a negotiation chat, the ransomware gang claims to have stolen 1.5 TB of files and is demanding $7 million not to publish the data and provide a file decryptor.

As proof that they stole data, the threat actors shared a PDF file indicating it is a scanned passport for a JVCKenwood employee.

Since providing proof of data theft, there has been no further contact from the JVCKenwood representative indicating that the company will likely not pay a ransom.

Conti is a ransomware family believed to be operated by the TrickBot threat actor group and is commonly installed after networks are compromised by the TrickBot, BazarBackdoor, and Anchor trojans.

The ransomware gang has been responsible for a wide range of attacks over the years, including high-profile attacks against the City of Tulsa, Ireland's Health Service Executive (HSE), Advantech, and numerous health care organizations.

More recently, the Conti gang faced some controversy after a disgruntled affiliate leaked the ransomware operation's attack playbook, giving law enforcement and researchers insight into their tactics.

Last week, a joint report between the FBI, CISA, and NSA warned of escalating Conti ransomware attacks.

BleepingComputer has contacted JVCKenwood with questions regarding the attack but has not heard back at this time.
